Considerations for Managing IoT Cybersecurity and Privacy Risk

Wednesday, July 11, 2018 | National Institute of Standards and Technology (NIST) Administration Building 101, 100 Bureau Drive, Gaithersburg, MD

The National Institute of Standards and Technology (NIST) Cybersecurity for the Internet of Things (IoT) Program supports the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed. By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

There has been broad support for NIST to provide guidance for federal agencies on how to secure their IoT within our Federal Information Security Management Act (FISMA) responsibilities. While agencies are aware that IoT affects cybersecurity and privacy risks, there remain questions about how to manage these risks.

NIST's Cybersecurity for IoT Program is drafting guidance for federal agencies on common high-level cybersecurity and privacy risks for IoT. NIST is interested in hearing practitioners' insights on managing cybersecurity and privacy risks to their IoT systems, using tools like the Cybersecurity Framework and NIST Special Publication (SP) 800-53 to help manage that risk, and specific feedback on what the use of these tools would look like.

Considerations for Managing IoT Cybersecurity and Privacy Risk

Wednesday, July 11, 2018 | National Institute of Standards and Technology (NIST)
Administration Building 101, 100 Bureau Drive, Gaithersburg, MD

Time	Topic
7:30 AM	**Registrant Check-In** | NIST cafeteria is available to attendees
8:30 AM	**Opening Remarks** | *Green Auditorium* Charles Romine | *Director, Information Technology Lab, NIST* Katerina Megas | *Program Lead, NIST Cybersecurity for IoT Program* Naomi Lefkovitz | *Senior Privacy Policy Advisor, NIST Privacy Engineering Program*
9:15 AM	**IoT General Model | Green Auditorium** Eric Simmon | *Senior Scientist, Cyber Infrastructure Group, NIST*
10:00 AM	**Break** | NIST cafeteria is available to attendees
10:15 AM	**Breakout Session #1** **Risk Considerations for the IoT General Model** | *Portrait Room* The IoT General Model describes what IoT is, focusing on its capabilities. This breakout will discuss the cybersecurity and privacy risk considerations from these capabilities and the challenges in addressing these risk considerations. **Applying IT Cybersecurity and Privacy Controls to IoT** | *West Square* There are numerous concerns about relying on existing IT cybersecurity and privacy controls for IoT, from the lack of controls built into many IoT devices to the negative impact some controls may cause to the physical world. This breakout session will highlight these concerns and explore how compensating controls can be leveraged to mitigate risk. **IoT Baselines, Profiles, and Overlays** | *Green Auditorium* Stakeholders have expressed a strong interest in cybersecurity and privacy baselines for IoT, such as minimum sets of SP 800-53 controls to be used for all IoT devices. This discussion will focus on opportunities to create IoT baselines, including Cybersecurity Framework profiles and SP 800-53 overlays, and examine possible candidates for inclusion in baselines. **Managing Privacy Risk for IoT** | *Lecture Room B* Privacy and cybersecurity overlap in areas such as protecting the confidentiality of PII, but there are also privacy concerns without cybersecurity implications. This breakout will focus on how to identify and manage IoT-specific privacy risks.
11:30 AM	**Lunch** | NIST cafeteria is available to attendees
12:30 PM	**Breakout Session #2 |** *See above for descriptions* **Risk Considerations for the IoT General Model** | *Portrait Room* **Applying IT Cybersecurity and Privacy Controls to IoT** | *West Square* **IoT Baselines, Profiles, and Overlays** | *Green Auditorium* **Managing Privacy Risk for IoT** | *Lecture Room C*
1:45 PM	**Break** | NIST cafeteria is available to attendees
2:00 PM	**Worked Examples Discussion** | *Green Auditorium*
3:00	**Recap and Next Steps** | *Green Auditorium*
3:30 PM	**Adjourn** | *Green Auditorium*